PORTABLE BIODATA PROTECTED DATA STORAGE UNIT

Field of Invention

This invention relates to a portable data storage unit which is capable of storing and easily transporting large amounts of data and which is disposed with a biometrics protected security and encryption function such that access to the data stored in the device is secured and available only to authorised users who provide the required biometric parameters.

Background

Biometrics parameters which may be utilised to secure access to data stored in the device include personal bio-behaviour or bio-characteristics such as fingerprint minutiae, voice characteristics, iris recognition, facial features and the like.

At this time there are no storage devices which are able to utilise a very broad range of biometrics parameters to secure access to data held in memory. This invention defines a complete bio protected portable data storage methodology which can utilise biometrics parameters such as finger print minutiae, voice vocal trace, eye iris, facial features and the like. Further there are no data storage devices which utilise the encryption methodology of generating an encryption key based on individual biometric parameters and a factory preset pointer to secure data. The use of such polynomial encryption appending function provides a degree of security which is not available with known data storage devices.

Summary of the Invention

A portable data storage device includes a biometrics recognising apparatus which comprises a biometric sensor and a biometrics processing engine. The storage device further includes a memory storage facility, a micro controller and a communications interface to enable the storage device to communicate with a host computer, an access control unit, a bioparameters storage unit, a combination encryption key generation means, a device code generation means, a bioencryption engine for encryption and decryption and a data processing unit.

The biometrics recognising apparatus is able to acquire the necessary biometric parameters from users and store the same in a storage means disposed within the device and which information can be used to permit access to the data stored in the storage means to authorised users only.

The biometrics sensor is reversibly connected to the biometrics processing engine. The biometrics processing engine is interconnected with an access control decision unit and a bioparameters storage unit. The bioparameters storage unit and the biometric processing engine are also interconnected with a combination encryption key generation means which is itself connected with a device code generation means. The access control unit is interconnected with a micro controller and a bioencryption engine unit which is itself interconnected with the memory storage means. The bioencryption engine is also reversibly interconnected with a data processing unit which is itself connected to the micro controller. The micro controller is reversibly connected to the communications device and thus to a host computer.

The biometrics sensor and biometrics processing engine are capable of

receiving, recognising, processing, identifying and verifying the desired biometric parameters from end users.

The device enables data to be transferred between a host computer and the storage device by a standard communications port employing standard data transfer protocols such as USB, UART, PCMCIA, Compact Flash, Fire-Wire and the like. The communications interface provides a channel between a host computer and the portable storage device which enables data to be sent to and retrieved from the device.

The biometrics processing engine comprises a processor capable of processing a digital signal and which engine is able to perform computations and calculations based on a set of predefined algorithms to generate a reference database in respect of the biometrics parameters.

The biometrics sensor comprises a sensing apparatus capable of receiving and recognising a variety of biometric data from a user such as fingerprint data, voice data, iris data, facial data or the like. The sensing apparatus may be active or passive and may incorporate one or more of optical, capacitive, electric field, laser, infra red or magnetic technology.

The biometrics sensor acquires the desired biometrics parameters from the user and these parameters are processed by the biometric processing engine in accordance with predefined algorithms and generate a reference database in respect of the said biometric data, which may be stored in the storage means.

Users biometric parameters are stored in the bioparameters storage unit pending

encryption. The biometric parameters are encrypted by the bioencryption engine using the biometric parameters and a factory preset parameter.

The storage means which may be volatile or non-volatile is capable of reversibly receiving and storing data for multi read/write applications.

The micro controller comprises a processor which incorporates the communications interface protocol and provides a gateway for data to be stored and retrieved from the storage means. The micro controller may also be disposed with a bioencryption algorithm. The bioencryption processing is based on the users biometrics information and this encrypted information acts as key to permit access to the data. The encryption process makes use of two parameters namely a factory preset parameter and the individual biometric parameter input by the user to create an encryption key for the encryption process. Such encryption key will be pointed and accessible by a pointer called the encryption pointer. Both the encryption and decryption pointers are the same and they complement each other.

Access can also be further secured with device identification to provide both bioencryption and system protection.

Data input by a user can be secured in accordance with the chosen biometric parameters and thus access to the stored data is limited only to those users who are enrolled as authorised users.

Enrollment of biometric data is carried out in respect of each authorised user. Each such user presents his/her required biometrics parameters to the biometrics

sensor disposed in the device. The said biometric parameters are scanned and processed by the biometrics processing engine in accordance with predefined encryption algorithms. The scanning and identification process may be repeated to ensure accuracy in recognition of the biometric parameter. The encrypted biometric parameter is then stored in the storage means and must be re-presented to the scanner to enable access to the data. The bioencryption is based on the users biometric information as the basic encryption key and in combination with device identification provides data and system protection. The further advantage of such encryption is that it is not possible to manually open the device, remove the storage means and gain access to the data via other commercial readers.

Brief Description of the Drawings

The invention will now be described by reference to the figures.

Figure 1 is a system functional block diagram and operational flowchart.

Figure 2 is a functional flow chart of proprietary data bioencryption scheme.

Description of the Preferred Embodiments

Figure 1 shows the relationship of the various components of the data storage device and the operational flowchart interconnecting the components. The device (1) may be connected to a host computer (100) via a communications interface (2). Data from the device can be uploaded to and downloaded from host computer through the communications interface (2). Data is stored in the storage means (3) and access to this data requires the correct biometric input from the biometrics scanner (4). The desired biometrics parameters are

presented to the biometrics scanner which reads the said data. This data is then processed by the biometrics processing engine (6) which is in connection with the biometrics sensor (5), the biometrics parameters storage unit (7) and the access control decision unit (8).

The access control decision unit evaluates the data processed by the biometrics engine and decides whether to grant access to the data stored in the memory means within the device. Such decision will be based on the degree and accuracy of the match between the input biometrics information and the biometrics template and parameters stored within the device.

If access right is granted, an encryption pointer will be generated for the encryption or decryption of the data information depending on whether it is a write or read process respectively.

The biometrics parameters storage unit (7) is interlinked to an encryption key generator (9) which is in turn interlinked to the bioencryption engine which encrypts and decrypts the data. Encrypted biometric data is then stored in the memory means (3).

In practice the user would enroll his/her biometric data by presenting such data to the biometric scanner (4). The biometric sensor (5) would read the data and transfer the data to the biometrics processing engine.

The data is then encrypted by the bioencryption engine processing the data in accordance with the encryption key generated by the device code generation means (12). The encrypted biometric data is then stored in the memory means

(3).

The encryption process makes use of two parameters namely a factory preset parameter and the individual biometric parameter input by the user to create an encryption key for the encryption process. Such encryption key will be pointed and accessible by a pointer called the encryption pointer. Both the encryption and decryption pointers are the same and complement each other.

Access to data stored in the device would require the user to present his/her biometric data to the scanner (4). The scanner reads the biodata presented. The said biodata is then analysed by the access control decision unit (8). The access control decision unit evaluates the data to establish whether the biodata is in conformity with the enrolled biodata stored in the memory means. If the biodata is acceptable the bioencryption engine (10) generates a decryption key to allow the user access to the data. Data can then be accessed through the communications interface (2) via the host computer (100).

Figure 2 sets out the functional flow chart of biodata encryption scheme. At the start of the process biometric information is input into the device via the scanner (101). This information is processed by the biometric sensor (102). The data is then verified (103) by the biometric processing engine. If the data is not verified further biometric data may be requested. If however the biometric data is verified the encryption key generation means prepares an encryption pointer (104). The encryption process makes use of two parameters namely a factory preset parameter (107) and the individual biometric parameter input by the user to create an encryption key for the encryption process. Such encryption key will be pointed and accessible by a pointer called the encryption pointer. Both the encryption and decryption pointers are the same and they complement each

other.

The encryption key, in respect of the presented biodata, which is stored in the memory means (105) is then retrieved. The encryption key is then added to the biodata (106) and the biodata is then decrypted (108) by the bioencryption engine.

Successful decryption enables the user to access data stored in the memory means (109) of the device via the communications interface (110).